UNITED STATES PATENT AND TRADEMARK OFFICE

**UNITED STATES DEPARTMENT OF COMMERCE**
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/750,529 | 12/31/2003 | Kevin R. Driscoll | 256.197US1 | 5548 |

128 7590 07/10/2008
HONEYWELL INTERNATIONAL INC.
101 COLUMBIA ROAD
P O BOX 2245
MORRISTOWN, NJ 07962-2245

| EXAMINER | |
|---|---|
| YALEW, FIKREMARIAM A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 07/10/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/750,529 | **Applicant(s)**<br>DRISCOLL, KEVIN R. | |
| | **Examiner**<br>Fikremariam Yalew | **Art Unit**<br>2136 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 April 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

1. The office action is in replay to an amendment filed on 04/07/2008. Claims 1-35 are pending.

### *Response to Arguments*

2. Applicant's arguments filed 0n 04/07/2008 have been fully considered but they are not persuasive.

3. The applicant argued that the prior art does not teach the use of an ephemeral value as a cryptographic key to generate a digital signature or hash. The examiner disagree and points out the prior art teach generating a digital signature of the data based on the ephemeral value (See Grawrok 0028-0029,0034 and see Fig 3 steps 310,315(i.e., produce ephemeral credential)).Further more the system in Grawrok relates to use of ephemeral value as a cryptographic key to perform encryption/decryption of data(i.e., the examiner reasonably interpreted using ephemeral value as a cryptographic key to perform encryption equivalent to use of an ephemeral value as a cryptographic key generate a digital signature or hash).The applicant also argued that the prior art do not teach or suggest generating a second digital signature with a cryptographic key having a value that is equal to the random number. The examiner disagree and points out generating a second digital signature with a cryptographic key having a value that is equal to the random number(See Grawrok 0033-0034& Fig 5 steps 530,540 ).The examiner maintains the previous office action rejection.

### *Claim Rejections - 35 USC § 102*

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-8,13-31are rejected under 35 U.S.C. 102(e) as being anticipated by Grawrock et al (herein after referred to as Grawrock) US Patent NO 2002/0080974 B2.

6. As per claim 1,13,24: Grawreock discloses a method/apparatus/a physical machine-readable medium comprising: receiving an ephemeral value from a challenging device (See 0029 and Fig 3 step 320(i.e., transmit ephemeral credential); retrieving data whose content is known to the challenging device (See 0017 and Fig 3 step 320(i.e., identity credential to the requestor)); generating a digital signature of the data based on the ephemeral value (See 0028-0029,0034 and see Fig 3 steps 310,315(i.e., produce ephemeral credential)); a cryptographic key having a value that is equal to the ephemeral value(See0033- 0034 and Fig 4 steps 410,420(i.e., ephemeral asymmetric public key matches EAPUK); and transmitting the digital signature to the device (See 0034 and Fig 3 step 320(i.e., transmit ephemeral credential).

7. As per claim 2,25: Grawreock discloses the method wherein receiving the ephemeral value from the challenging device comprises receiving a randomly generated number from the challenging device (See 0028,0030).

8. As per claim 3,26: Grawreock discloses the method wherein retrieving the data comprises retrieving at least part of application code (See 0017).

9. As per claim 4,27: Grawreock discloses the method wherein generating the digital signature of the data based on the ephemeral value comprises generating a one-way hash across the data with the cryptographic key having a value that is equal to the ephemeral value (See 0033-0034).

10. As per claim 5,28: Grawreock discloses a method comprising: receiving, into a response device, an ephemeral value from a challenge device (See 0029 and Fig 3 step 320); retrieving data from an address space in the response device, wherein the data is known to the challenge device and the response device (See 0017 and Fig 3 step 320); generating a hash across the data using the ephemeral value as a key of the hash (See 0028-0029,0034 and Fig 5 steps 510,520); and transmitting at least part of the hash to the challenge device(See 0034 and Fig 5 steps 500,510).

11. As per claim 6,29: Grawreock discloses the method further comprising generating a reduced hash based on the hash, wherein transmitting the ephemeral value and the at least part of the hash to the challenge device comprises transmitting the ephemeral value and the reduced hash to the challenge device (See 0033-0034 ).

12. As per claim 7,30: Grawreock discloses the method wherein retrieving the data from the address space in the response device comprises retrieving application code to be executed in the response device (See 0014,0017 ).

13. As per claim 8,31: Grawreock discloses the method wherein retrieving the data from the address space in the response device comprises retrieving configuration parameters of the response device (See Fig 3 step 320).

14. As per claim 10: Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating an application executable (See 0017,0021).

15. As per claim 11: Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating at least one security parameter (See Fig 3 step 320 ).

16. As per claim 12: Grawreock disclose the method wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature (See Grawreok 0033-0034 and Fig 4 steps 410,420).

17. As per claim 14: the combination of Johnson and Grawreock disclose the apparatus wherein the I/O logic is to receive the request for authentication from a challenge device, the I/O logic to transmit the cryptographic hash back to the challenge device (See Grawreock Fig 2 and 0033-0034).

18. As per claim 15: the combination of Johnson and Grawreock disclose the apparatus wherein the storage medium is a nonvolatile memory (See 0021-0022,0024).

19. As per claim 16: the combination of Johnson and Imai disclose further comprising a data selection logic to select less than all of the data, wherein the at least part of the data is the less than all of the data (See 0024,0028).

20. As per claim 17: the combination of Johnson disclose the apparatus wherein the data selection logic is to select less than all of the data based on a random number based selection of segments of the data (See 0028,0030-0031).

21. As per claim 18: Grawreock the apparatus wherein the data comprises an application to be executed in the apparatus (See 0017,0021).

22. As per claim 19: Grawreock discloses the apparatus wherein the data comprises at least one security parameter of the apparatus (See Fig 3 step 320).

23. As per claim 20: Grawreock discloses a challenge device to authenticate data presumably stored in a response device, the challenge device comprising: a storage medium to store a copy of the data presumed to be stored in the response device (See (See 0028,0030); a key generation logic to generate an ephemeral value (See 0025); an input/output (I/O) logic to output a request for authentication to a response device, wherein the request includes the ephemeral value, the I/O logic to receive a first digital signature from the response device in response to the request for authentication(See Fig 2 step 200 and 0029-0030); a signature logic to retrieve the copy of the data and the ephemeral value and to generate a second digital signature(See 0029-0030); and an authentication logic to compare the first digital signature to the second digital signature, wherein the data is authenticated if the first digital signature equals the second digital signature(See 0030 and Fig 5 steps 530,540).

24. As per claim 21: Grawreock discloses the challenge device wherein the ephemeral value comprises a randomly generated value (See 0028,0030 ).

25. As per claim 22: Grawreock discloses the challenge device wherein the data comprises application code to be executed by the response device (See 0014, 0017).

26. As per claim 23: Grawreock discloses the challenge device wherein the data comprises at least one configuration parameter of the remote device (See Fig 3 steps 320).

## *Claim Rejections - 35 USC § 103*

27. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

28. Claims 9-12,32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson, P. K.,et al(hereinafter referred as Johnson) (W0 00/18162) in view of Grawrock et al (herein after referred to as Grawrock) US Patent NO 2002/0080974 B2 .

29. As per claim 9,32: Johnson discloses a method comprising: authenticating data having predictable content and stored in an address space of a remote device, the authenticating comprising: generating a random number (See col 10 lines 20-33 ); transmitting the random number to a remote device presumably having the data (See col 6 lines 17-24 and Figs 2,3); receiving, from the remote device, a first digital signature that is representative of the data (See col 6 lines 25-33 and abstract );

Johnson does not explicitly teach generating a second digital signature with a cryptographic key having a value that is equal to based on the random number; and comparing the first digital signature to the second digital signature.

However Grawrock teaches generating a second digital signature with a cryptographic key having a value that is equal to based on the random number(See 0028-0029,0034 and see Fig 3 steps 310,315) and comparing the first digital signature to the second digital signature(See 0033-0034& Fig 5 steps 530,540).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Johnson with in inorder to enhancing the security of the system.

30. As per claim 10,33: the combination of Johnson and Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating an application executable (See Johnson col 7 lines 1-3).

31. As per claim 11,34: the combination of Johnson and Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating at least one security parameter (See Johnson col 7 lines 1-3).

32. As per claim 12,35: the combination of Johnson and Grawreock disclose the method wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature (See Grawreok 0033-0034).

### *Conclusion*

**33. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew Art Unit 2136
07/07/2008
FA
/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136